

DISARM Content Security
for MS Exchange Online
User Manual

DISARM Content Security

for MS Exchange Online

Used by hundreds of thousands of users worldwide, DISARM is specially-built for securing content. It provides a multi-layered security pipeline, combining traditional threat analysis with the market's most advanced sandbox and Content Disarm and Reconstruction (CDR) technologies. This combination ensures all content is fully sanitized before it even reaches user devices -- no matter if it contains yet unknown or evasive malware. DISARM allows you to do so faster and with lower cost and complexity.

Table of Content

1. Features
2. Alert Emails
3. FAQ & Contact Info



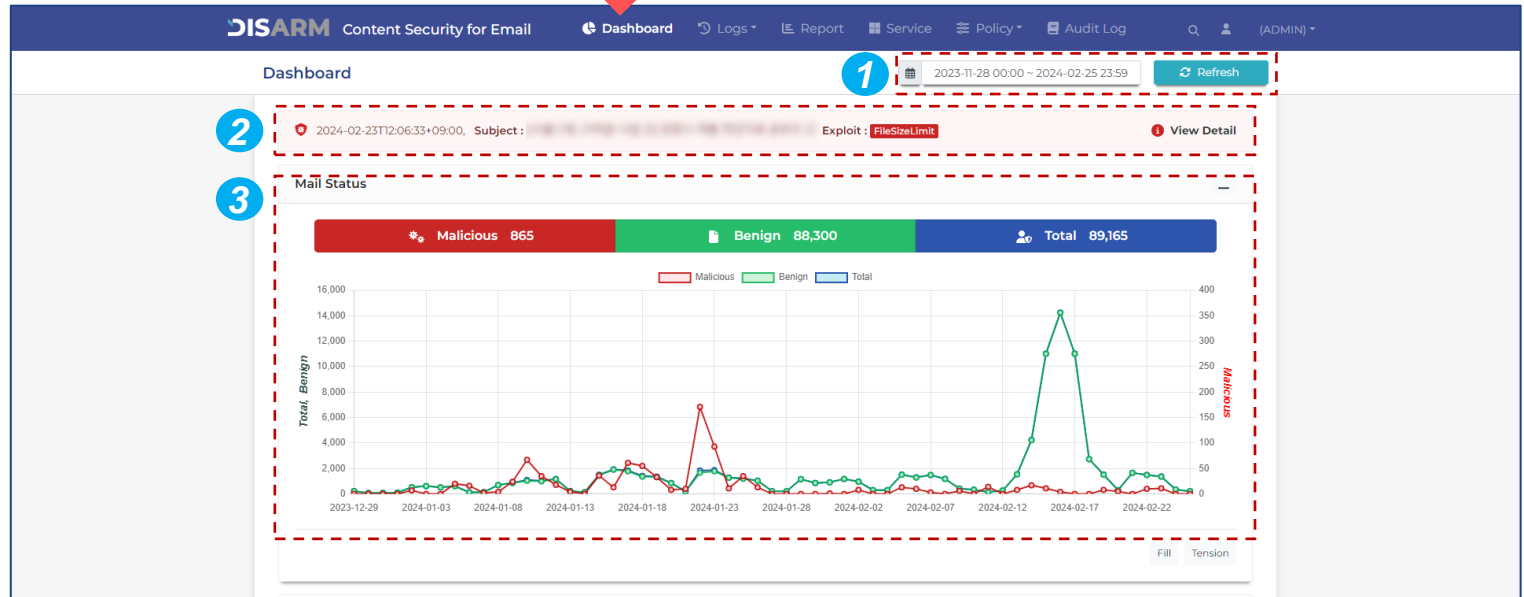
1. Features



Feature 1 “Dashboard”

Check your company’s email status at a glance. Simply set the date range and get the information you need.

1. Dashboard - Top page



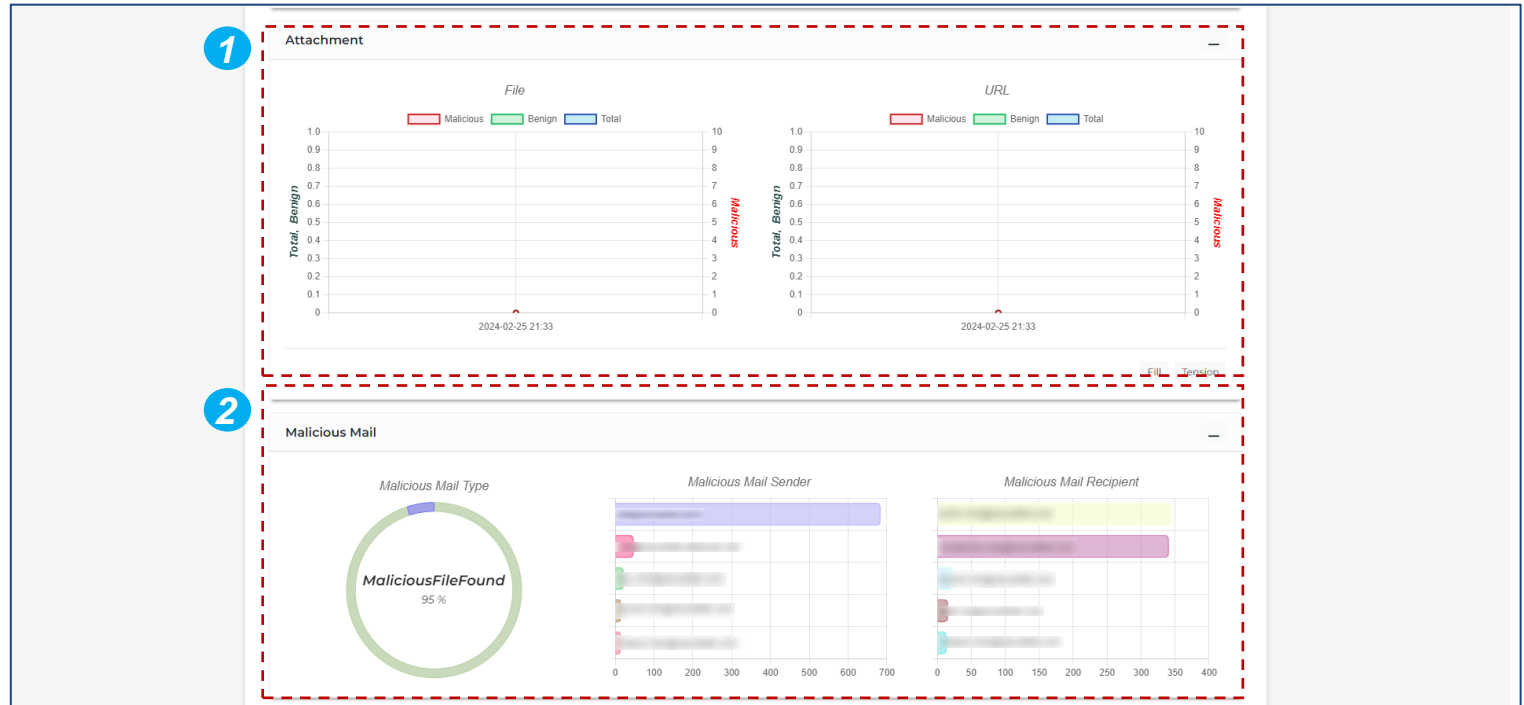
- 1 Set the period you want to check the overview status of email flow.
- 2 The most recent detected email information.
- 3 Check email status overview of the period you set.



Feature 1 “Dashboard”

Check your company’s email status at a glance. Simply set the date range and get the information you need.

1. Dashboard - Attachment, Malicious Mail



1 Check email status of the period you set by attachment types.

2 Check email status of the period you set by malicious email type.

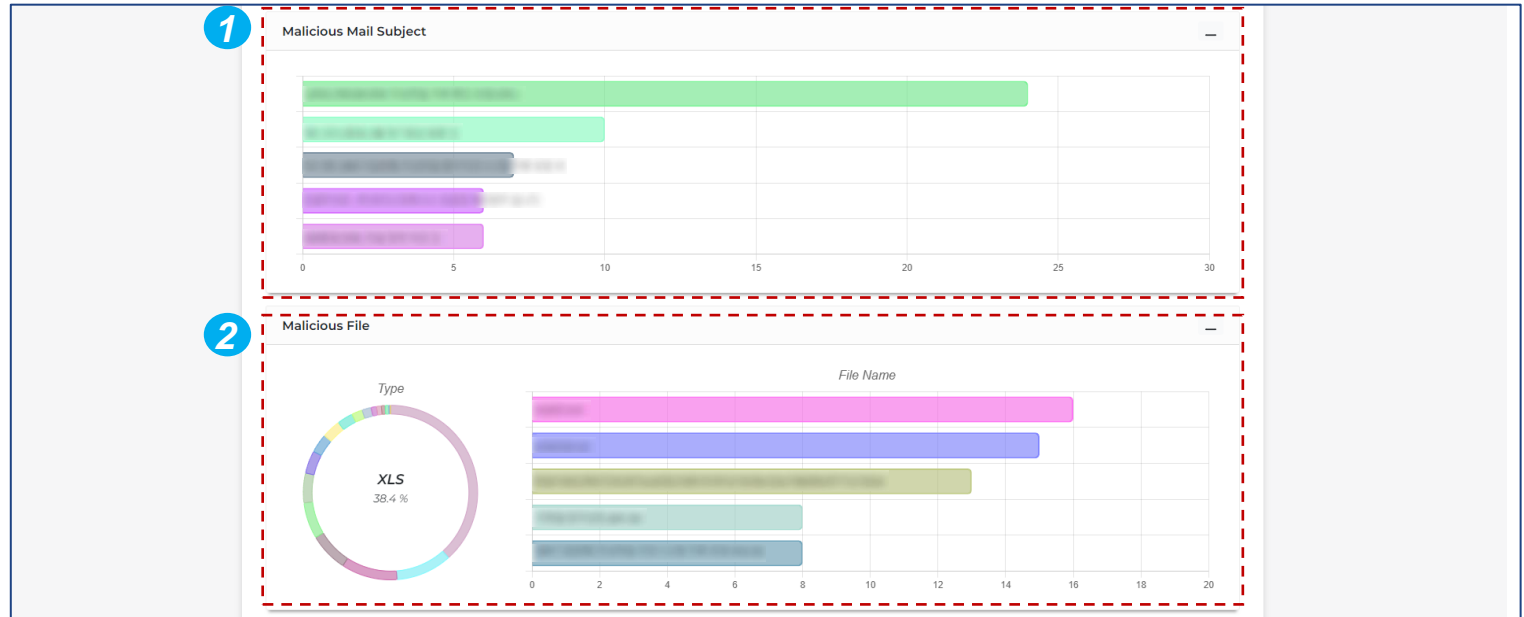
You can also check Top 5 malicious email sender and recipient list.



Feature 1 “Dashboard”

Check your company’s email status at a glance. Simply set the date range and get the information you need.

1. Dashboard - Malicious Mail Subject, Malicious File



1 Check Top 5 malicious email subject of the period you set.

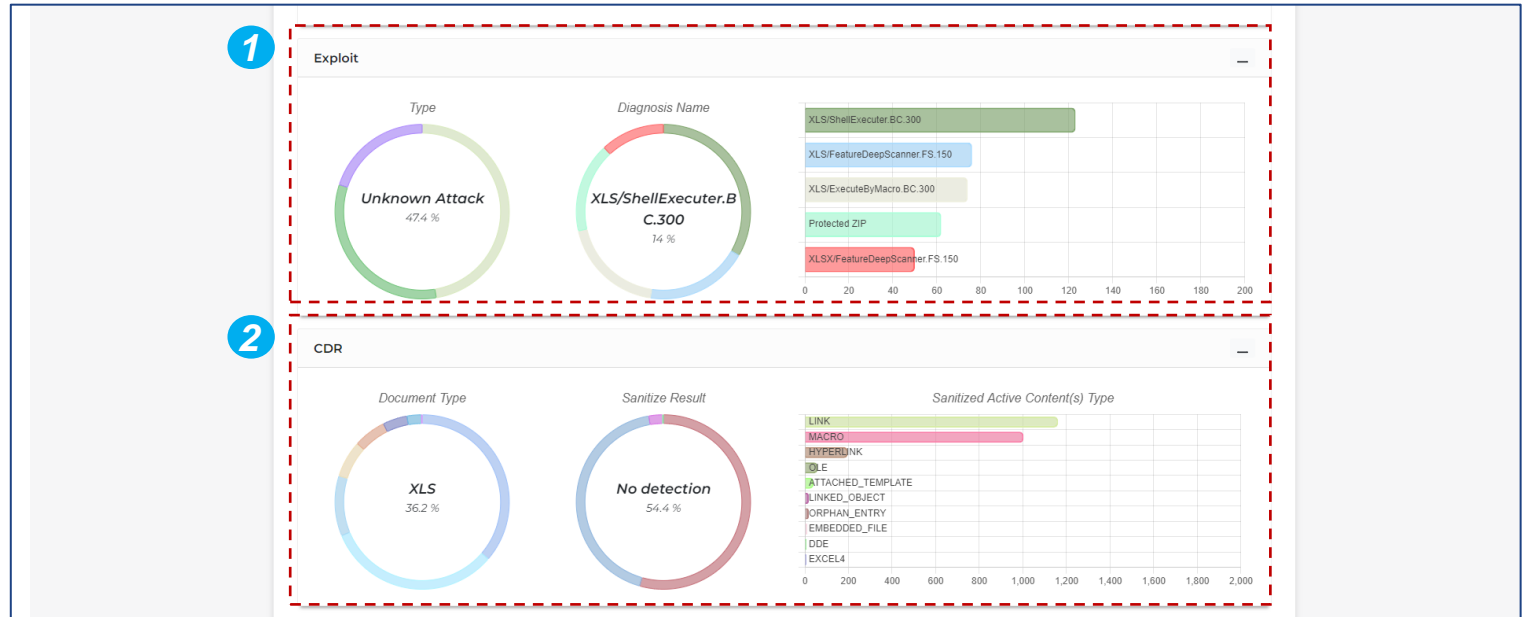
2 Check email status of the period you set by malicious file type.



Feature 1 “Dashboard”

Check your company’s email status at a glance. Simply set the date range and get the information you need.

1. Dashboard - Exploit, CDR



- 1 Check email status of the period you set by exploit type.
- 2 Check CDR (Content Disarm and Reconstruction) result statics of the attached document files.



Feature 2 “Logs - Email”

DISARM provides detailed analysis result. Via this log page, you can see all the incoming emails by each email, file or URL. For user’s privacy, email body contents are ONLY available for detected as ‘Malicious’.

2. Logs - Email

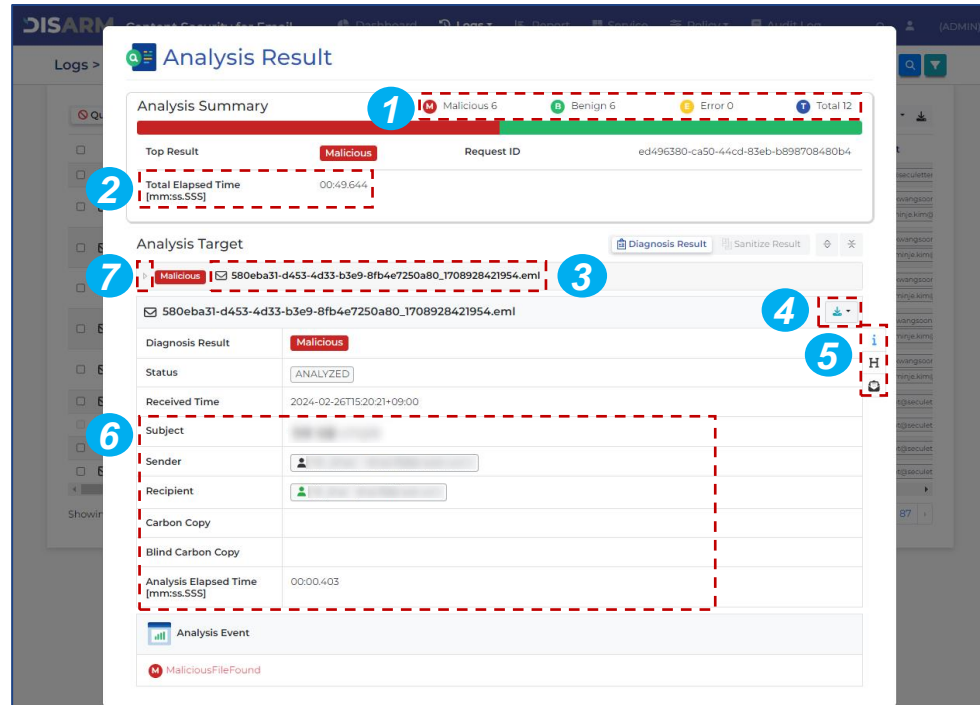
- 1 Set the period or filters you want to see the logs.
*Filter: Sender, Recipient, Subject and Diagnosis Name
- 2 'Quarantine' displays only for 'Malicious Email'. Click 'All' will show the all-diagnosis result.
- 3 Use these buttons to 'Refresh page', 'Fullscreen view', 'Select log list columns', 'Change text size', and 'Export the list as CSV'.
- 4 Click each email log to see the detailed diagnosis result.
- 5 Check the emails and click 'Send mail' to release to recipient's inbox.
*Paper plane icon is appeared for released mail.



Feature 2 “Logs - Email”

By clicking one of the email from the log list, you can check the detailed diagnosis result information.

2. Logs - Email (Result Popup Page for Email)



- 1 The number indicates the diagnostic result of the targeted analysis component.
- 2 The total time taken by DISARM to receive the email to send it to the mail server.
- 3 Unique ID given by MTA.
- 4 Download the EML file as a file or zip.
- 5 Check EML info, headers and body.
- 6 Check email subject, sender, recipient and analysis time for the EML.
- 7 Click the little arrow to see the attached files and its results.
(Continue in the next page)



Feature 2 “Logs - Email”

For attached document files, DISARM provides very detailed information. Check out 'Assembly Instruction Analysis' for dynamic features and the experience of having your own malware analyst.

2. Logs - Email (Result Popup Page for Attachment)

The screenshot displays the DISARM analysis interface. The top section shows the 'Analysis Result' summary, including the top result, total elapsed time, and analysis target. A red dashed box labeled '1' highlights the file name or URL. A red dashed box labeled '2' highlights the 'VT LINK' button. A red dashed box labeled '3' highlights the 'Analysis Data' section. A red dashed box labeled '4' highlights the 'Analysis Events' section. A red dashed box labeled '5' highlights the 'Dynamic Features' section, specifically the 'Reverse-engineering' sub-section.

The 'Analysis Data' section is expanded to show 'Dynamic Features > Reverse-engineering'. It includes the following information:

- Reverse-engineering:** DDE(Dynamic Data Exchange) Execution
- Static Features:**
 - Reverse Code Extraction: Attach process name: EXCEL.EXE (1588)
 - IoC: Module: excel.exe
 - MetaData: Register: C.W.D., E.I.E.
 - Bundle Files: Memory data: 000000004300400044002E00 4500580045002000 81006C006300
 - Extracted Code: Payload: 00.EHE /C calc
 - File Feature: Disassembly x86: Description: Execute command by using DDE(Dynamic Data Exchange). Detection: Benign
 - Embedded Image: CreateProcessInternalW API parameter check
 - Embedded Files: Attach process name: EXCEL.EXE (1588)
 - Module: kernel32.dll
 - Register: C.W.D., E.I.E.
 - Memory data: 000000004300400044002E00 4500580045002000
 - Payload: 00.EHE /C calc
 - Disassembly x86: Description: Inspected CreateProcessInternal function parameter. Detection: Benign

- 1 Click on the file name or URL to view the detailed analysis results.
- 2 Click 'VT LINK' to compare the diagnosis result with VirusTotal or download the attached file.
- 3 View various file information.
- 4 Click on each analysis event to see what component of the file is performing what behavior.
- 5 DISARM provides even more detailed analysis data extracted by its dynamic and static engines. Dynamic features are from 'Assembly Instruction Analysis' technique.

*Each feature is enabled only if the analyzed file has the relevant component.



Feature 2 “Logs - Email”

CDR (Content Disarm and Reconstruction) is one of the great advantages of DISARM to make your business communication better and more secure.

DISARM CDR removes any suspicious or potential threats inside the files such as Hyperlink, Visual Basic Macro, JavaScript, Dynamic Data Exchange, etc.

With DISARM CDR, you can open the file with confidence!

2. Logs - Email (Result Popup Page for Sanitize Result)

The screenshot displays the 'Analysis Result' interface. At the top, there's an 'Analysis Summary' with a progress bar showing 6 Malicious, 6 Benign, 0 Error, and a Total of 12. Below this, the 'Top Result' is 'Malicious' and the 'Request ID' is 'ed496380-ca50-44cd-83eb-b898708480b4'. The 'Total Elapsed Time' is '00:49:644'. A red dashed box highlights the 'Sanitize Result' button (1). Below the summary, a list of files is shown with their status: '함흥 성품.pptx' (Benign), 'https://...' (Benign), 'https://...' (Malicious, Not run), 'http://www...' (Benign), 'http://www...' (Malicious, Not run), 'http://www...' (Benign), and 'https://...' (Benign). A red dashed box highlights the file name '함흥 성품.pptx' (2). Below the file list, the 'Sanitize Result' for '함흥 성품.pptx' is shown as 'Success'. The 'Message' is 'CDR Process Success'. The 'MDS' is '82500d803b92d2ab9153048f4885ffa', 'SHA1' is '9531431842533df4c4f4b65d74c5948bd8dc1ef', and 'SHA256' is '4b4ddeb4ee3794a6de582546e6fd7ad632073a62c1f13e2ebf1e137b51a50afa'. The 'File Extension' is 'PPTX'. A red dashed box highlights the 'CDR Report' button (4). Below the file list, the 'CDR Report' is shown, including a 'Sanitized' section with a 'File Overview' and a 'Content Disarm & Reconstruction' section. The 'Content Disarm & Reconstruction' section shows a table of linked objects that were sanitized.

NO	Type	Sanitized Information	No. of Detection
1	XML_NODE	https://...	1
2	XML_NODE	https://...	1

- 1 Click on ‘Sanitize Result’ to check CDR result of each file.
- 2 The left button shows ‘Diagnosis Result’ and the right button shows ‘Sanitize Result’.

Status	Description
Success	CDR processing is finished.
Not run	File(s) is not of a supported extension type.
No detection	File(s) there is no active content to be removed.
Failure	Mainly means that the file(s) is incorrect format file(s).
No support	Mainly means that the file(s)’ format is too old version to process CDR.
Recompress	Only displayed for compressed file(s) after CDR success. All recompressed files’ extension will be modified as ‘.zip’.

*For more details, please see the ‘Sanitize Result’ log.

- 3 Click on the file name to view the detailed CDR results.
- 4 View the detailed CDR report. It shows what DISARM CDR removed from the original file.



Feature 2 “Logs - File”

DISARM provides detailed analysis result.

Via this log page, you can see all the incoming attached files.

2. Logs - File

Date & Time	First Submit	Diagnosis Result	Sanitize Result	File Name
2024-01-19T05:01:30+09:00	2024-01-19T05:01:45+09:00	Malicious	Success	
2024-01-18T20:03:47+09:00	2024-01-18T20:04:17+09:00	Malicious	Success	
2024-01-18T20:03:46+09:00	2024-01-18T20:03:47+09:00	Malicious	Success	
2024-01-18T15:01:36+09:00	2024-01-18T15:02:05+09:00	Malicious	Success	
2024-01-18T15:01:35+09:00	2024-01-18T15:01:36+09:00	Malicious	Success	
2024-01-18T15:01:33+09:00	2024-01-18T15:01:33+09:00	Malicious	Success	
2024-01-18T15:01:33+09:00	2024-01-18T15:01:50+09:00	Malicious	Success	
2024-01-18T11:01:37+09:00	2024-01-18T11:02:02+09:00	Malicious	No detection	
2024-01-18T11:01:36+09:00	2024-01-18T11:02:02+09:00	Malicious	No detection	
2024-01-18T04:01:29+09:00	2024-01-18T04:01:29+09:00	Malicious	Success	
2024-01-18T04:01:29+09:00	2024-01-18T04:01:56+09:00	Malicious	Success	

- 1 Set the period or filters you want to check the logs.
*Filter: Analysis Result, File Type, CDR Status, File Name, Diagnosis Name
- 2 Use this buttons to 'Refresh page', 'Fullscreen view', 'Select log list columns', 'Change text size, and 'Export the list as CSV'.
- 3 Click each file log to see the detailed diagnosis result.
*Result page is same as p.20.



Feature 2 “Logs - URL”

DISARM provides detailed analysis result.
Via this log page, you can see all the URL
inside the email body or attached files.

2. Logs - URL

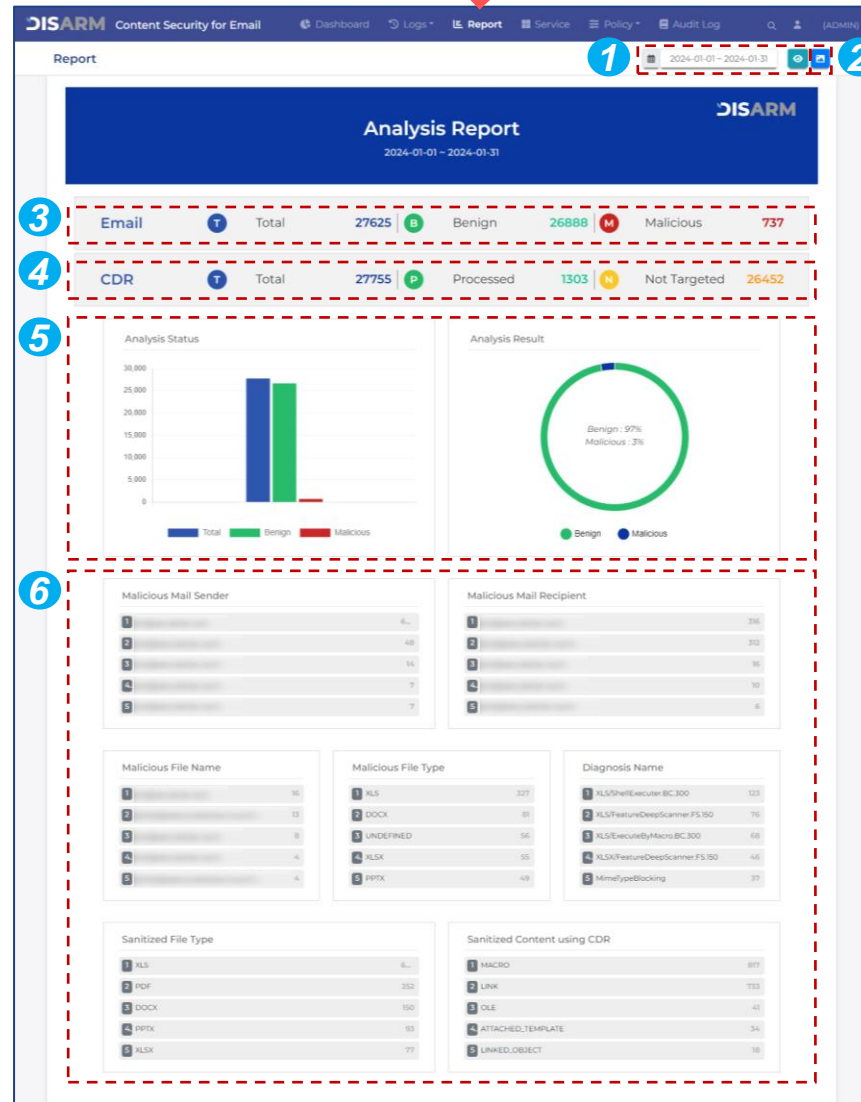
Date & Time	Diagnosis Result	URL	Analysis Elapsed Time [mm:ss.SSS]
2024-02-22T22:02:02+09:00	Malicious		00:00.601
2024-02-22T22:02:01+09:00	Malicious		00:00.801
2024-02-22T22:02:00+09:00	Malicious		00:00.400
2024-02-22T22:01:59+09:00	Malicious		00:00.601
2024-02-22T21:02:04+09:00	Malicious		00:00.400
2024-02-22T21:02:02+09:00	Malicious		00:00.401
2024-02-19T12:21:28+09:00	Malicious		00:00.801
2024-02-19T12:13:02+09:00	Malicious		00:00.601
2024-02-19T12:13:02+09:00	Malicious		00:00.605
2024-02-16T14:39:24+09:00	Malicious		00:00.402

- 1 Set the period or filters you want to check the logs.
*Filter: Analysis Result, URL, Diagnosis Name
- 2 Use this buttons to 'Refresh page', 'Fullscreen view', 'Select log list columns', 'Change text size, and 'Export the list as CSV'.
- 3 Click each URL log to see the detailed diagnosis result.
*Result page is same as p.20.

Feature 3 “Report”

Need help creating an email security status report? Just come to report page and easily create your exclusive report!

3. Report



- 1 Specify the date range and click the button to the right to generate a report. (Max. 31 days)
- 2 Click the button to open the report in a new window and save it as a PDF or print it as a hard copy.
- 3 Summary of detection and analysis result.
- 4 Summary of CDR process result.
- 5 Statistic chart of detection and analysis result.
- 6 Top 5 malicious and CDR information by categories.



Feature 4 “Policy”

Create your own blacklist and whitelist based on certain file hash.

4. Policy - File Hash



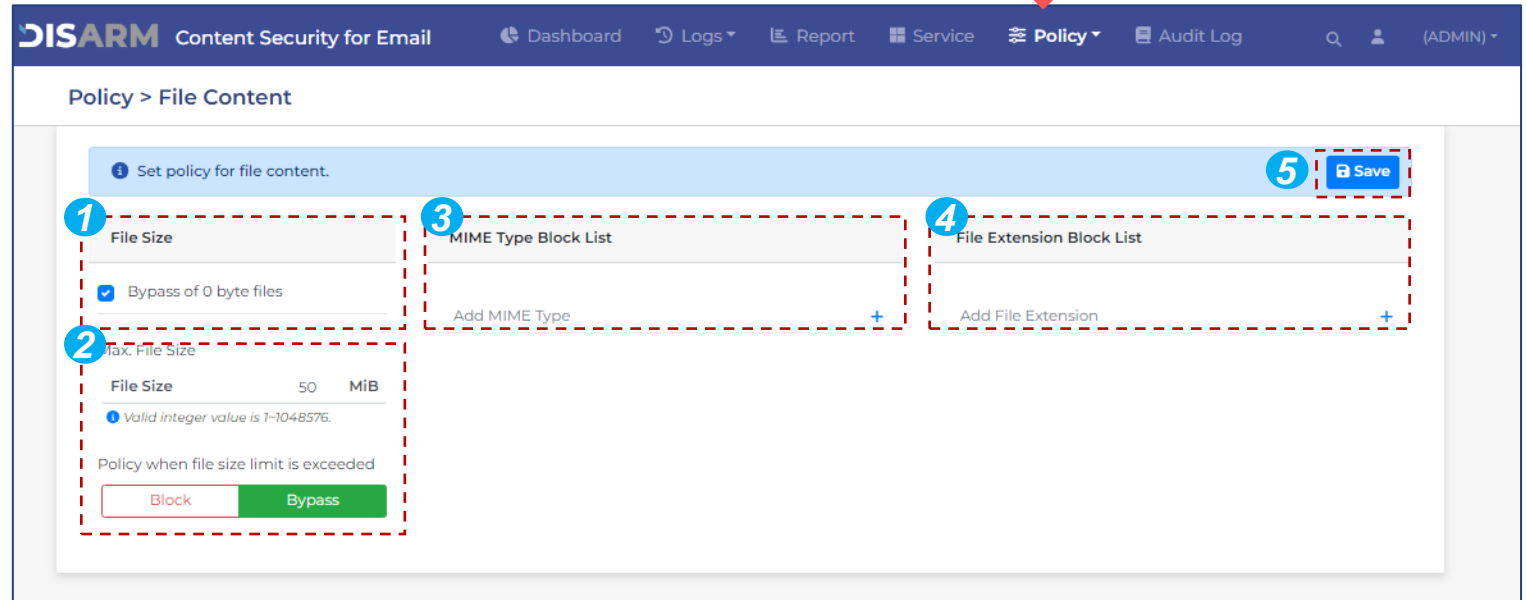
- 1 Select 'Blocked List' to add file hash to block email with the blacklisted file. And select 'Allowed List' to add file hash to pass email with the whitelisted file.
- 2 Use these buttons to 'Refresh page', 'Fullscreen view', 'Select columns', 'Upload a List of File Hash as CSV', and 'Export the list as CSV'.
- 3 Displays the file hash information that entered in 4 below.
*Hash Algorithm is filled automatically.
- 4 Insert MD5, SHA1, SHA256 and also leave the description to figure out what it is.
- 5 Don't forget to click 'Save' button to reflect the file hash information in the list.



Feature 4 “Policy”

Set up detailed policy based on various file information.

4. Policy - File Content



- 1 Check the box to bypass 0-byte files.
- 2 Set the maximum file size to analyze. You can also decide to block or bypass all files that exceed the maximum file size.
- 3 Add certain MIME type to block.
- 4 Add certain file extension to block.
- 5 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

To analyze executable files such as EXE or DLL, DISARM offers various settings upon your preference.

4. Policy - Executable File

- 1 Select whether to block the executable file or analyze it for bypass/blocking.
- 2 Check the box if you want to block hidden executable files.
Check the box if you want to block double extensions for executable files.
- 3 Create whitelist to bypass certain file digital signature by inserting signature and click the '+' button. This means that you block all other signatures that are NOT registered in this list.
- 4 Created whitelist to bypass certain executable file extensions signature by inserting extension and click the '+' button. This means that you block all other executable file extensions that are NOT registered in this list.
- 5 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

When an email containing encrypted compressed file(s) is received, DISARM attempts to decrypt the files using a pre-registered ‘Common Used Password’ dictionary. If there is no matching password, DISARM sends a password request email to the recipient.

*See page 27 for password request email.

*To proceed above, the Compressed File policy must be set to ‘**BLOCK**’.

4. Policy - Password Protected File ✓

DISARM Content Security for Email

Dashboard Logs Report Service Policy Audit Log (ADMIN)

Policy > Password Protected File

1 Set policies for password-protected compressed/document files. (If decompress with a common password is not possible, the set policy is followed) Save

Document file	Compressed file	Common Used Passwords
BLOCK	BLOCK	donald
BYPASS	BYPASS	monkey
BYPASS when the document file is protected with password.	ANALYZE	shadow
	ANALYZE when the compressed file is protected with password.	Tq2w3e4r
		sunshine
		111111
		aa123456
		123456789
		qwerty
		abc123
		Showing 1 to 10 of 73 rows 10 rows per page 1 2 3 4 5 ... 8
		Add Password +

- 1 Select whether to block or bypass password protected document files.
*Feature for analyzing password protected document files will be available in 2024 Q2.
- 2 Select one of the options for password protected compressed files such as ZIP, EGG,7Z, etc.
- 3 Register commonly used password and make DISARM automatically unzip the file for analysis.
*Around 70 passwords are initially given.
- 4 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

Don't be bothered by phishing URLs.
DISARM thoroughly scans not only URLs
in the email body, but also URLs in
attachments.

4. Policy - URL Analysis



- 1 Select one of the options to activate or not the URL analysis.
*Skip: Deactivate / Extract URL: Activate
- 2 Select one of the target file type options for URL extraction.
- 3 Add URL(s) to skip analysis process.
- 4 Add URL(s) to block. Emails containing block listed URL(s) will be blocked.
- 5 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

Experience the lowest document reconstruction failure rate with DISARM's CDR.

With DISARM CDR, you can confidently open document files without the potential threats they contain.

4. Policy - CDR

- 1 Select one of the options to activate or not the CDR feature.
*OFF: Deactivate / ON: Activate
- 2 Set the maximum file size to sanitize.
- 3 Set the maximum file depth to sanitize.
*This is for embedded or OLE files.
- 4 Set the policy for files that could not be sanitized.
*CDR Failure mainly occurs when the file(s) is incorrect format file(s).
- 5 Set CDR policy per file extension.
*OFF: Deactivate / ON: Activate
- 6 Set CDR policy per file version.
*To see the exact file extensions, hover over the extension category.
- 7 Select active content to remove.
- 8 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

DISARM provides very detailed incoming email information for admin, but sometimes there are email users who handle your company's confidential information, like your CEO, CFO and more.

Keep everyone's inbox secure but hide confidential information for VIPs!

4. Policy - Masking

- 1 Select one of the options to activate or not the Masking feature.
*OFF: Deactivate / ON: Activate
- 2 Check the box on the left to also hide information from malicious emails.
- 3 Register the email address to which you want to apply the masking policy.
- 4 Don't forget to click the 'Save' button whenever you make any changes to the page.



Feature 4 “Policy”

Be suspicious of senders you haven't heard from before or in a long time. Especially if the email contains URLs or attachments.

DISARM provides profiling banner feature to alert recipients to new emails.

4. Policy - Profiling

- 1 Select one of the options to activate or not the Masking feature.
*OFF: Deactivate / ON: Activate / MONITORING: Keep logs for profiling feature, but do not display banner to users.
- 2 Select period to apply for profiling policy.
*The first time you use DISARM, even if you enable profiling, the banner will not be displayed until after the time period you select on the left.
- 3 Write a sentence that you want to appear in the top banner of the user's email.
- 4 Don't forget to click the 'Save' button whenever you make any changes to the page.

Feature 5 “Audit Log”

It displays logs of what has been done in this admin console during the specified time period. You can see all console activity by who and when in detail.

5. Audit Log

The screenshot shows the 'Audit Log' page in the DISARM Content Security for Email admin console. The page title is 'System > Audit Log'. The breadcrumb navigation includes 'Dashboard', 'Logs', 'Report', 'Service', 'Policy', and 'Audit Log'. The user is identified as '(ADMIN)'. The main content area displays a table of audit events with columns: Date & Time, Event ID, Event Status, Extension, User, IP, and Data. The table contains 10 rows of log entries, including successful logins, policy setting changes, and mail release requests. At the bottom, there is a pagination control showing 'Showing 31 to 40 of 301 rows' and a '10 rows per page' dropdown. A red checkmark is positioned above the screenshot, and two red dashed boxes with numbers 1 and 2 highlight specific UI elements: box 1 highlights the date range filter and search icons, and box 2 highlights the table action icons (Refresh, Fullscreen, Select columns, Text size, Export as CSV).

- 1 Set the period or filters you want to check the logs.
*Filter: Event ID, Event Status, Extension, User, IP
- 2 Use this buttons to 'Refresh page', 'Fullscreen view', 'Select log list columns', 'Change text size, and 'Export the list as CSV'.

2. Alert Emails

Alert Email 1 “Malicious Mail”

"You are protected!" Your users receive this email when malicious emails are proactively blocked before they reach the recipient's inbox.

1. Malicious Mail Detection for Recipients

General Information

1	Title		
	Sender		2
3	Recipient		
	CC		4

Details

#	Item	Total Count	Malicious Count
1	URL	1	1

Please contact your administrator for more details on the quarantined email.

DISARM

- 1 The title of the malicious email.
- 2 Sender of the malicious email.
- 3 Recipient of the malicious email.
- 4 Carbon copy recipient(s) of the malicious email.
- 5 Summary of the malicious content(s) in the email.



Alert Email 2 “Password Request”

Recipients will receive this email to submit the appropriate password for the protected compressed file(s) that DISARM is holding for analysis. Once the password is submitted, DISARM will begin the analysis process to determine whether or not the compressed file(s) are malicious.

2-1. Password Request Email

General Information

1 Title
2 Sender
3 Recipient
4 CC

Details

#	Item	Total Count	Malicious Count
1	File	2	

Compressed files exist that have not been analyzed.

6 **Why should I click the button and insert password?**
For your system safety, all files coming through email must be analyzed. However, password-protected compressed file cannot be analyzed without the password. If it is malicious the email will be blocked and if it is benign the email will be delivered to your inbox soon. If you are suspicious on this alert email, please contact your IT team to check.

7 **PROVIDE PASSWORD FOR ATTACHED COMPRESSED FILE**

Please contact your administrator for more details on the quarantined email.

- 1 The title of the malicious email.
- 2 Sender of the malicious email.
- 3 Recipient of the malicious email.
- 4 Carbon copy recipient(s) of the malicious email.
- 5 Summary of the malicious content(s) in the email.
- 6 Description of the need for and process of providing a password.
- 7 Button to open a new page to enter the password.



Alert Email 2 “Password Request”

Recipients will receive this email to submit the appropriate password for the protected compressed file(s) that DISARM is holding for analysis. Once the password is submitted, DISARM will begin the analysis process to determine whether or not the compressed file(s) are malicious.

2-2. Malicious Mail Detection for Recipients

The screenshot shows the top portion of an email interface. At the top is a dark blue header with the DISARM logo and a globe icon. Below the header is a white section titled "Password Needed". A light blue information bar contains the text: "i The mail received contains a password-protected compressed file among the attached files. You can check your email address and enter a password to diagnose malicious files." Below this is a search bar with a blue "1" icon on the left, the text "Recipient | Enter the email address.", and a blue "OK" button on the right. A red dashed box highlights the search bar and the "OK" button.

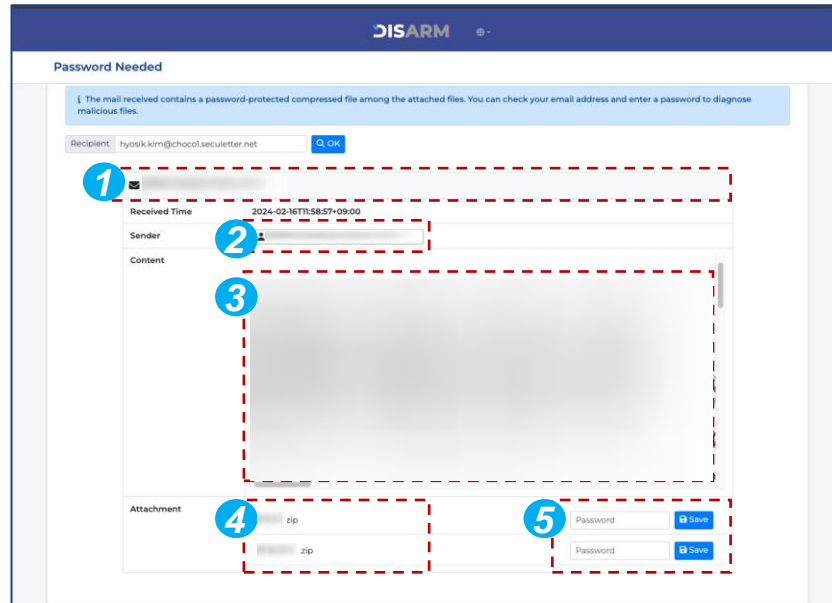
- 1 Verify the recipient's email address, then click 'OK'.



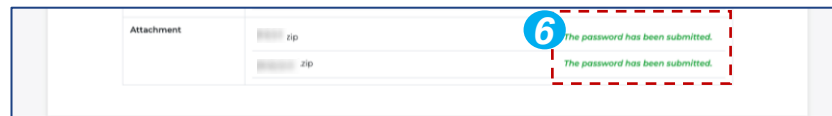
Alert Email 2 “Password Request”

Recipients will receive this email to submit the appropriate password for the protected compressed file(s) that DISARM is holding for analysis. Once the password is submitted, DISARM will begin the analysis process to determine whether or not the compressed file(s) are malicious.

2-3. Malicious Mail Detection for Recipients



- 1 The title of the email.
- 2 Sender of the email.
- 3 Email body content.
- 4 Attached compressed file's name.
- 5 Password submit area.
- 6 After entering the password, section 5 changes to show the message.



3. FAQ & Contact Info

FAQ

Q. How does installing the DISARM Content Security service apply Zero Trust CDR to Microsoft 365?

A: The email received by the subscriber is sent to the DISARM Content Security service, which analyzes the email body and attachments, and then performs the content disarming for malicious content. Once the process is complete, the safe email is forwarded to the subscriber with a notification bar at the top of the email body.

Q. What if my organization already has Microsoft security in place?

A: Even if you have a security feature provided by Microsoft 365, we recommend adopting DISARM Content Security to enhance your organization's security. Because Microsoft 365 security features provide signature-based security, it is difficult to detect and block unknown new and variant malicious code and ransomware that bypasses security features. In comparison, the DISARM Content Security service detects and proactively blocks both known and unknown security threats, making Microsoft 365 more secure.

FAQ

Q. How do I install the DISARM Content Security service?

A: Download and install the application from the [Microsoft App Source DISARM Content Security page](#). The installation will be complete in a few minutes. For more information, visit the Microsoft App Source DISARM Content Security page.

Q. Who should I contact for further advice?

A: Please email us as global@seculetter.com anytime. Our team will get back to you as soon as possible.



DISARM

©2024 SecuLetter Co., Ltd.
All rights reserved.